METHOD OF GUARANTEEING USERS' ANONYMITY AND WIRELESS LOCAL AREA NETWORK (LAN) SYSTEM THEREFOR

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention relates to wireless Local Area Network (LAN) system. More particularly, the present invention relates to a method of guaranteeing a user's anonymity and a wireless LAN system therefor, by using a temporary address generated from a unique Media Access Control (MAC) address as a source address or a destination address.

2. Description of the Related Art

[0002] Generally, a wireless LAN system consists of an ad-Hoc network where a plurality of terminals, each of which includes a wireless Network Interface Card (NIC), are connected to each other and independently to wired LANs, and an infrastructure network where wireless terminals are connected to wired LANs through wireless access nodes. In an infrastructure network, a wireless cell Basic Service Set (BSS) is formed centering on one wireless access node. The wireless access node has the same functionality as a cellular phone station and connects all wireless terminals in the BSS to a LAN.

[0003] FIG. 1 illustrates a conceptual scheme showing the structure of a wireless LAN system of a general infrastructure network. A wireless LAN system as shown in FIG. 1 consists of a wireless access node 11 and four

wireless terminals 13, 15, 17, and 19. The wireless access node 11 is connected to a wired network, such as very-high-speed Internet lines or private lines, and performs access arbitration between wireless terminals. The four wireless terminals 13, 15, 17, and 19 form a BSS and include wireless LAN cards respectively. The wireless LAN cards installed respectively in the first to fourth wireless terminals 13, 15, 17, and 19 have MAC addresses MAC Addr1 to MAC Addr4 corresponding to the first to fourth wireless terminals 13, 15, 17, and 19.

[0004] The unique MAC addresses MAC Addr1 to MAC Addr4 allocated to the respective wireless LAN cards of the first to fourth wireless terminals 13, 15, 17, and 19 are used as source addresses or destination addresses when sending and receiving data packets between the first through fourth wireless terminals 13, 15, 17, and 19 through the wireless access node 11. That is, to transmit a data packet (for example, a protocol data unit (PDU)) to one wireless terminal among the first to fourth wireless terminals 13, 15, 17, and 19, the wireless access node 11 sends transmission frames 12, 14, 16, and 18, each of which contain a unique MAC address (i.e., a MAC address among the first to fourth MAC addresses MAC Addr1 to MAC Addr4) of a wireless terminal representing the destination address. The address is placed in the header of the data packet (PDU) to be transmitted. On the other hand, each of the first to fourth wireless terminals 13, 15, 17, and 19 compares the MAC

address corresponding thereto with the destination addresses contained in the headers of the transmission frames 12, 14, 16, and 18 sent from the wireless access node 11. If a destination address is identical to the MAC address corresponding to a wireless terminal, the corresponding wireless terminal accepts the frame. If no match is made, the frame is dropped over the network.

[0005] MAC addresses used for data communication between wireless terminals through wireless access nodes are unique values allocated upon manufacturing wireless LAN cards. The MAC address is not varied and also not encoded. Accordingly, MAC addresses are exposed during data communication so that anonymity of a user using a corresponding MAC address can not be guaranteed. Thus, a user using the corresponding MAC address may be easily tracked. That is, by merely monitoring unique MAC addresses, private user information about network access state, network access time, etc., may be outflowed, and more seriously, if any unique MAC address is exposed, a greater risk exists for malicious users eavesdropping at the link layer. Further, attack possibility to encryption channels is increased in long-running monitoring.

[0006] As described above, since it is necessary to guarantee a user's anonymity so that information about a user of a wireless LAN system is not

leaked to objects other than a permitted entity, the conventional wireless LAN system of the infrastructure network has many security problems.

SUMMARY OF THE INVENTION

[0007] The present invention provides a method for guaranteeing a user's anonymity in a wireless Local Area Network (LAN) system by using a temporary address randomly selected from a temporary address set that contains mapping to a Media Access Control (MAC) address as the source address or the destination address upon transmitting data packets between a wireless access node and wireless terminals.

[0008] The present invention further provides a wireless LAN system for guaranteeing a user's anonymity by using a temporary address generated from a unique MAC address.

[0009] According to a feature of an embodiment of the present invention, there is provided a method of guaranteeing users' anonymity in a wireless LAN system, the method including: (a) creating a plurality of temporary address sets, each of which corresponds to a unique Media Access Control (MAC) address of a wireless terminal, and transmitting each temporary address set to the corresponding wireless terminal, and (b) performing data packet transmissions between a wireless terminal and a wireless access node using a temporary address selected from the temporary address set corresponding to the wireless terminal as a source address or a destination address.

[0010] In the method above, the wireless access node may create the temporary address sets, each of which preferably consists of N (where N is an integer greater than or equal to two) temporary addresses using a MAC address contained in an access or authentication request message transmitted from a corresponding wireless terminal.

[0011] In the method above, in (a), the wireless access node may encode the temporary address sets using a predetermined encryption key for each temporary address set, and may respectively transmit the encoded temporary address sets to the corresponding wireless terminals. Each encryption key may be created upon authentication of the corresponding wireless terminal.

[0012] In the method above, (b) may further include (b1) a first addressing, which is performed in the wireless access node, and generates a temporary address as a destination address randomly selected from the temporary address set corresponding to a wireless terminal that is requesting authentication. Also, (b) may include (b2) a second addressing, which is performed in the wireless terminal, and generates a temporary address as a source address randomly selected from the temporary address set corresponding to the wireless terminal.

[0013] According to another feature of an embodiment of the present invention, there is provided a computer readable medium having embodied thereon a computer program for the method described above.

[0014] According to another feature of an embodiment of the present invention, there is provided a wireless Local Area Network (LAN) system of guaranteeing users' anonymity including a wireless access node, which creates a plurality of temporary address sets, each of which corresponds to a unique Media Access Control (MAC) address of a wireless terminal, and uses a temporary address selected from each temporary address set as a destination address, and at least one wireless terminal, which receives a temporary address set corresponding to a unique MAC address thereof from among the plurality of temporary address sets created in the wireless access node, and uses a temporary address selected from the received temporary address set as a source address.

[0015] In the system above, the wireless access node may create the temporary address sets, each of which consists of N (where N is an integer greater than or equal to two) temporary addresses, preferably using for each address set the MAC address contained in an access or authentication request message transmitted from the corresponding wireless terminal.

[0016] In the system above, the wireless access node preferably encodes the temporary address sets using a predetermined encryption key for each address set, and respectively transmits the encoded temporary address sets to the corresponding wireless terminals. Preferably, each encryption key is created upon authentication of the corresponding wireless terminal.

[0017] In the system above, the wireless access node may include a first memory, which stores the plurality of temporary address sets, each of which consists of N (where N is an integer greater than or equal to two) random addresses and is created corresponding to a unique MAC address, a first MAC address filter, which filters a unique MAC address from a source address of a data packet received from a corresponding wireless terminal by referring to the temporary address sets stored in the first memory, a destination address generation unit, which enables a temporary address set corresponding to the unique MAC address of the wireless terminal requesting authentication from among the temporary address sets stored in the first memory, generates a first random selection signal, generates a temporary address randomly selected from the enabled temporary address set, and uses the temporary address as a destination address, and a first random selection unit which randomly selects a temporary address from the temporary address set enabled in the first memory according to the first random selection signal generated in the destination address generation unit, and outputs the selected temporary address to the destination address generation unit.

[0018] The wireless terminal may include a second memory which receives a temporary address set from the wireless access node and stores the temporary address set corresponding to a unique MAC address of the wireless terminal, a second MAC address filter which determines whether a

destination address of a data packet received from the wireless access node is included in the temporary address set by referring to the temporary address set stored in the second memory, and generates a receipt enable signal according to a determination result, a source address generation unit, which generates a second random selection signal according to a source address request signal, generates a temporary address randomly selected from the temporary address set stored in the second memory, and uses the temporary address as a source address, and a second random selection unit which randomly selects a temporary address from the temporary address set stored in the second memory according to the second random selection signal generated in the source address generation unit, and outputs the selected temporary address to the source address generation unit.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019] The above and other features and advantages of the present invention will become more apparent to those of ordinary skill in the art by describing in detail preferred embodiments thereof with reference to the attached drawings in which:

[0020] FIG. 1 illustrates a conceptual scheme showing the structure of a general wireless Local Area Network (LAN) system;

[0021] FIG. 2 is a flow chart for describing a method of guaranteeing users' anonymity in a wireless LAN system according to a preferred embodiment of the present invention;

[0022] FIG. 3 illustrates a view for describing an operation relationship between a wireless access node and wireless terminals;

[0023] FIG. 4 is a block diagram showing a detailed structure of an addressing unit of the wireless access node in the wireless LAN system according to a preferred embodiment of the present invention; and

[0024] FIG. 5 is a block diagram showing a detailed structure of an addressing unit of the wireless terminal in the wireless LAN system according to a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0025] Korean Patent Application No. 2002-39155, filed on July 6, 2002, and entitled: "Method Of Guaranteeing Users' Anonymity And Wireless Local Area Network (Lan) System Therefor," is incorporated by reference herein in its entirety.

[0026] FIG. 2 is a flow chart for describing a method of guaranteeing users' anonymity in a wireless LAN system according to an embodiment of the present invention. The method of guaranteeing users' anonymity includes access step 21, authentication step 22, temporary address set generation step 23, temporary address set transmission step 24, and data packet

transmission step 25. FIG. 3 illustrates a view for describing the operation relationship between a wireless access node and wireless terminals. Signal transmissions between a wireless access node and a wireless terminal in the above-mentioned steps are illustrated in FIG. 3.

[0027] Now, the steps shown in FIG. 2 will be described in connection with FIGS. 1 and 3.

[0028] In the access step 21, if a first wireless terminal 13 requests access, access between the first wireless terminal 13 and a wireless access node 11 is performed. For performing this access, the first wireless terminal 13 transmits to the wireless access node 11 an access request message Association_Req containing its own unique MAC address MAC Addr1 as the source address (process 31 of FIG. 3). The wireless access node 11, which receives the access request message Association_Req, tries to access the first wireless terminal 13. If this access succeeds, the wireless access node 11 transmits to the first wireless terminal 13 an access success message Association_Resp containing the unique MAC address MAC Addr1 of the first wireless terminal 13 as the destination address (process 32 of FIG. 3).

[0029] In the authentication step 22, if a first wireless terminal 13 requests authentication, the wireless access node 11 performs authentication of the first wireless terminal 13. For performing this authentication, the first wireless

terminal 13 transmits to the wireless access node 11 an authentication request message Authentication_Req containing its own unique MAC address MAC Addr1 as the source address (process 33 of FIG. 3). The wireless access node 11, which receives the authentication request message Authentication_Req, performs an authentication of the first wireless terminal 13. If the authentication succeeds, the wireless access node 11 creates an encryption key. At this time, the wireless access node 11 transmits to the first wireless terminal 13 the encryption key in the authentication success message Authentication_Resp containing the unique MAC address MAC Addr1 of the first wireless terminal 13 as the destination address (process 34 of FIG. 3).

[0030] In the temporary address set generation step 23, the wireless access node 11 randomly transforms the unique MAC address MAC Addr1 of the first wireless terminal 13 contained in the authentication request message Authentication_Req, and creates a temporary address set consisting of N temporary addresses corresponding to the unique MAC address, wherein N is preferably an integer greater than or equal to two (process 35 of FIG. 3).

[0031] In the temporary address set transmission step 24, the temporary address set created in the wireless access node 11 is encoded using the encryption key created in the authentication step 22, and then is transmitted to

the first wireless terminal 13 using the unique MAC address MAC Addr1 of the first wireless terminal 13 as the destination address (process 36 of FIG. 3).

[0032] In the data packet transmission step 25, whenever data communication is performed between a first wireless terminal 13 and wireless access node 11, a temporary address is randomly selected from a temporary address set and assigned to the data packet as a source address or destination address. That is, when the first wireless terminal 13, which receives an authentication success message Authentication_Resp and a temporary address set from the wireless access node 11, tries to transmit a data packet PDU to the wireless access node 11, the first wireless terminal 13 addresses as the source address a temporary address, i.e., a first temporary address Taddr1, randomly selected from the N temporary addresses in the temporary address set and transmits the data packet PDU (process 37 of FIG. 3). On the other hand, when a data packet PDU is transmitted from the wireless access node 11 to the first wireless terminal 13, a temporary address, i.e., a third temporary address Taddr3, randomly selected from the N temporary addresses in the temporary address set, is set as the destination address and the data packet PDU is transmitted (process 38 of FIG. 3).

[0033] FIG. 4 is a block diagram showing a detailed structure of an addressing unit 40 of the wireless access node 11 in the wireless LAN system of the present invention. The addressing unit 40 includes a memory 41, a MAC

address filter 43, a destination address generation unit 45, and a random selection unit 47, for addressing the destination addresses used in the data packet transmission step (step 25) described with reference to FIG. 3.

[0034] Referring to FIG. 4 in addition to FIGS. 1-3, operations of the addressing unit 40 will now be described. After a wireless access node 11 completes authentication of a first wireless terminal 13, a temporary address set which consists of N temporary addresses randomly created corresponding to a unique MAC address of the first wireless terminal 13, are stored in memory 41. At this time, a temporary address set is created corresponding to a unique MAC address for each wireless terminal requesting authentication and the temporary address sets are stored in the form of a look up table in memory 41.

[0035] A MAC address filter 43 works together with memory 41 when a data packet is transmitted from the first wireless terminal 13 to the wireless access node 11. The destination address generation unit 45 and the random selection unit 47 work together with memory 41 when a data packet is transmitted from the wireless access node 11 to the first wireless terminal 13. Operations of these components will be described in detail as follows.

[0036] The MAC address filter 43 receives a source address (SA) extracted from the data packet transmitted from the first wireless terminal 13, and attempts to discover a temporary address set including a temporary address

matching the source address by referring to the plurality of temporary address sets stored in memory 41. If the temporary address set is found, a unique MAC address corresponding to the temporary address set is extracted and transmitted to any layers requiring it.

[0037] The destination address generation unit 45 receives the unique MAC address of the first wireless terminal 13 obtained in the access/authentication steps, finds a temporary address set corresponding to the received unique MAC address among the plurality of temporary address sets stored in memory 41, activates the found temporary address set, and then outputs a random selection signal to a random selection unit 47.

[0038] The random selection unit 47 randomly selects a temporary address from the temporary address set activated in memory 41, depending on the random selection signal, and outputs the selected temporary address to the destination address generation unit 45. The destination address generation unit 45 sets the temporary address received from the random selection unit 47 as the destination address (DA), and outputs the destination address (DA).

[0039] That is, whenever data packets are transmitted from the wireless access node 11 to the first wireless terminal 13, each data packet has a different destination address from the others. This applies equally to other wireless terminals in a BSS (Basic Service Set).

[0040] FIG. 5 illustrates a block diagram showing a detailed structure of an addressing unit 50 of the first wireless terminal 13 in the wireless LAN system according to the present invention. The addressing unit 50 includes a memory 51, a MAC address filter 53, a source address generation unit 55, and a random selection unit 57, for addressing the source addresses used in the data packet transmission step 25 described with reference to FIG. 3.

[0041] Referring to FIG. 5 in addition to FIGS. 1-3, operations of the addressing unit 50 will now be described. Temporary address sets transmitted from the wireless access node 11 are stored in the memory 51. Only one temporary address set corresponding to a unique MAC address of the first wireless terminal 13 is stored in the memory 51.

[0042] The MAC address filter 53 works together with the memory 51 when a data packet is transmitted from the wireless access node 11 to the first wireless terminal 13. The source address generation unit 55 and the random selection unit 57 work together with memory 51 when a data packet is transmitted from the first wireless terminal 13 to the wireless access node 11. Operations of these components will be described in detail as follows.

[0043] The MAC address filter 53 receives a destination address (DA) extracted from the data packet transmitted from the wireless access node 11, determines whether a temporary address allocated to the destination address (DA) is included in the temporary address set stored in memory 51, and

outputs a receipt enable signal indicating receipt of the data packet, according to the determination result. That is, the first wireless terminal 13 receives the data packet sent from the wireless access node 11 when a temporary address allocated to the destination address (DA) is included in the temporary address set stored in memory 51.

[0044] The source address generation unit 55 outputs a random selection signal to the random selection unit 57 when receiving a source address request signal, in order to transmit a data packet from the first wireless terminal 13 to the wireless access node 11. The random selection unit 57 randomly selects a temporary address from the temporary address set stored in memory 51, according to the random selection signal, and outputs the selected temporary address to the source address generation unit 55. The source address generation unit 55 sets the temporary address provided from the random selection unit 57 as the source address (SA), and outputs the source address (SA) to the wireless access node 11.

[0045] That is, whenever data packets are transmitted from the first wireless terminal 13 to the wireless access node 11, each data packet has a different source address from the others. This applies equally to all other wireless terminals in a BSS.

[0046] The above-described preferred embodiments may be embodied as computer programs and may also be embodied on a general-purpose digital

computer for executing the computer programs using a computer readable medium. The computer readable medium may include storage media such as magnetic storage media (e.g., ROM's, floppy discs, hard discs, etc.), optically readable media (e.g., CDROMs, DVDs, etc.), and carrier waves (transmissions over the Internet).

[0047] As described above, according to the present invention, it is possible to prevent a MAC address from being exposed during data communication, thereby guaranteeing a user's anonymity, by using a temporary address selected from a temporary address set that contains mappings to a unique MAC address. The temporary address is used as a source address or a destination address upon data communication between a wireless access node and a wireless terminal.

[0048] Also, by using a temporary address randomly selected from a temporary address set, it is possible to prevent the outflow of private information and reduce the risk of attack by malicious users. The temporary address is used as the source address or destination address upon data communication between a wireless access node and a wireless terminal, so that whenever a data packet is transmitted, a different source address or a different destination address is used.

[0049] Preferred embodiments of the present invention have been disclosed herein and, although specific terms are employed, they are used and are to be

interpreted in a generic and descriptive sense only and not for purpose of limitation. Accordingly, it will be understood by those of ordinary skill in the art that various changes in form and details may be made without departing from the spirit and scope of the present invention as set forth in the following claims.